REMARKS / ARGUMENTS

In response to the Office Action dated January 14, 2004, Applicant respectfully requests the Office to enter the following amendments and consider the following remarks. By this amendment, Applicant amends claim 7 and cancels claim 27 without prejudice. Claims 1-26 are now pending in this application. Authorization is hereby given to charge any fees (e.g., extension fees) associated with this response to Deposit Account No. 06-0916.

In the Office Action, the Examiner: (i) objected to the Information Disclosure Statement in that legible copies of the non-patent literature were allegedly not provided; (ii) objected to an informality in the specification; (iii) rejected claims 7, 10-11, 13 and 27 under 35 U.S.C. § 102(e) as being unpatentable over U.S. Patent No. 6,047,242 to Benson ("Benson"); and (iv) rejected claims 1-6, 8, 9, 12 and 14-26 under 35 U.S.C. § 103(a) as being unpatentable over Benson in view of U.S. Patent No. 6,009,543 to Shavit ("Shavit").

Information Disclosure Statement

The Examiner has stated that the Information Disclosure Statement filed March 21, 2003 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because the non-patent literature could not be found. Applicant hereby re-submits the references in question, in an Information Disclosure Statement filed herewith.

Objection to the Specification

Applicant thanks the Examiner for noting the inadvertent error in the specification. Applicant has amended the specification in the manner recommended by the Examiner.

35 U.S.C. § 102(e) Rejections

Claims 7, 10-11, 13, and 27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Benson. *See* Office Action, page 3, paragraph 3.1. Claim 7, as amended, recites a computer system that includes (i) an insecure arrangement for using an application and (ii) a trusted element. The trusted element selects a portion of the application and issues a challenge that requests a response from the insecure arrangement, the response providing a computation of at least one value based on the selected portion of the application.

Applicant respectfully submits that Benson does not teach or suggest a system such as that described in Applicant's claim 7. Unlike Applicant's claim 7, in which a challenge is generated based on a predetermined portion of an application, Benson describes a fundamentally different challenge/response mechanism that involves the validation of public keying material. The keying material is not **a portion of the application**, as recited in Applicant's claim 7, but instead appears to be a specially created file that includes information (e.g., a public key) identifying the user of the application, but otherwise bearing no direct relationship to the content of the application

itself. In contrast, the challenge response mechanism recited in Applicant's claim 7 makes direct use of portions of the application itself, thus providing a mechanism for ensuring that the application has not been tampered with.

In addition, Applicant has amended claim 7 to clarify that the trusted element that generates the challenge is part of the same computer system that makes use of the application and issues the response to the challenge. In contrast, the cited portions of Benson describe a system that makes use of a remote license server to perform one of the roles in the challenge/response protocol. That is, the challenge/response mechanism described in Benson derives part of its security by making use of a license server that is remote from the computer system on which the application is being run. In contrast, Applicant's claim 7 describes a system in which the entire challenge/response process is executed locally, using a trusted element residing on the same computer system that is running the application.

For at least these reasons, Applicant respectfully submits that claim 7 is not anticipated by Benson. Claims 8-13 are dependent on claim 7, and are thus allowable for at least the reasons set forth above in connection with claim 7.

35 U.S.C. § 103(a) Rejections

The Examiner rejected claims 1-6, 8, 9, 12 and 14-26 under 35 U.S.C. § 103(a) as being unpatentable over Benson in view of Shavit.

Claim 1 recites a method of verifying an electronic item by, *inter alia*, presenting a secure credential comprising predefined plural subsets of the electronic item and

corresponding cryptographic hashes; randomly selecting one of the predefined plural subsets and computing the corresponding cryptographic hash; and testing whether the computed cryptographic hash corresponds to a cryptographic hash in the presented credential.

Applicant respectfully submits that neither Benson nor Shavit, alone or in combination, teach or suggest the invention claimed by Applicant.

First, as the Examiner acknowledges, Benson does not show, "randomly selecting one of the predefined plural subsets" (*see* Office Action at page 5, paragraph 4.2, lines 10-12). Moreover, as set forth above, Applicant respectfully submits that Benson does not teach or suggest a method in which an electronic item such as an application program is verified by examining predefined subsets of the electronic item itself.

Second, Applicant respectfully disagrees with the Examiner's characterization of Shavit as "analogous art [that] teaches randomly selecting one of the predefined plural subsets" (*Id.*, citing Shavit column 11 lines 49-57). The cited portion of Shavit reads:

> In step 108, a subset of the *program inputs* is selected in accordance with a predetermined criteria. For example, a random subset of the *program inputs* may be selected in accordance with a random seed provided by generator 72 (FIGS.3 and 3A). As another example, the program code may be traced into paths and selected *subsets of inputs* may be those which affect a particular one or more paths, such as the longest

or shortest path or the path having the most or least input dependencies.

Shavit, column 11, lines 49-57 (emphasis added).

Subsets of an electronic item's *inputs* are not the same as subsets of the electronic item itself, not to mention the additional step of randomly selecting one of the subsets of the electronic item as a basis for forming a secure credential. The invention described in Applicant's claim 1 is designed and configured for verifying an electronic item in an insecure environment, it is not clear how the teachings of Benson combined with the teachings of Shavit would render such a result obvious. Moreover, even if one wished to combine these two references, there is no reasonable probability of success since the random selection of an electronic item's inputs would not provide the necessary verification of the actual electronic item, as claimed by Applicant.

Claims 2-6 are dependent on claim 1, and are thus allowable for at least the reasons set forth above in connection with claim 1.

The Examiner also rejected independent claim 14 under 35 U.S.C. § 103(a) as being unpatentable over Benson in view of Shavit for reasons similar to those provided in connection with claim 1. Claim 14 recites a method for certifying an electronic item such a computer application, wherein portions of the electronic item are randomly selected, a cryptographic value corresponding to each of the selected portions is computed, and a credential defining each of the randomly selected portions and the corresponding cryptographic values is specified.

Applicant respectfully submits that neither Benson nor Shavit, alone or in combination, teach or suggest the invention claimed by Applicant.

First, as the Examiner acknowledges, Benson does not show, "randomly selecting plural portions of the electronic item" (*see* Office Action at page 7, lines 1-4). Moreover, Applicant respectfully disagrees with the Examiner's characterization of Benson, for reasons similar to those set forth above in connection with claim 1. In particular, Applicant respectfully submits that Benson does not teach or suggest a method in which an electronic item such as an application program is certified using selected portions of the electronic item itself.

Second, Applicant respectfully disagrees with the Examiner's characterization of Shavit as "analogous art [that] teaches randomly selecting plural portions of the electronic item" (*Id.,* citing Shavit, column 11, lines 49-57). The cited portion of Shavit reads:

> In step 108, a subset of the *program inputs* is selected in accordance with a predetermined criteria. For example, a random subset of the *program inputs* may be selected in accordance with a random seed provided by generator 72 (FIGS.3 and 3A). As another example, the program code may be traced into paths and selected *subsets of inputs* may be those which affect a particular one or more paths, such as the longest or shortest path or the path having the most or least input dependencies.

Shavit, column 11, lines 49-57 (emphasis added).

Subsets of an electronic item's *inputs* are not the same as portions of the electronic item itself. A credential created in the manner described in Applicant's claim 14 could be used to verify an electronic item in an insecure environment. It is not clear how the teachings of Benson combined with the teachings of Shavit would render such a result obvious. Moreover, even if one wished to combine these two references, there is no reasonable probability of success, since the selection of the electronic item's inputs would not provide a mechanism to verify the content of the electronic item itself, unlike the method claimed by Applicant.

Claims 15-19 are dependent on claim 14, and are thus allowable for at least the reasons set forth above in connection with claim 14.

The Examiner also rejected independent claims 20 and 21 under 35 U.S.C. § 103(a) as being unpatentable over Benson in view of Shavit for the same reasons provided in connection with claim 14. For reasons similar to those set forth above in connection with claim 14, Applicant respectfully disagrees.

First, Applicant respectfully disagrees with the Examiner's characterization of Benson. In particular, Applicant respectfully submits that Benson does not teach or suggest a mechanism for certifying an electronic item such as an application program using selected portions of the electronic item itself.

Second, Applicant respectfully disagrees with the Examiner's characterization of Shavit as "analogous art [that] teaches randomly selecting plural portions of the electronic item" (*Id.*, citing Shavit, column 11, lines 49-57). Instead, as previously

indicated, the cited portion of Shavit at most describes the random selection of a subset of a program's inputs. Subsets of an electronic item's *inputs* are not the same as portions of the electronic item itself. A credential created using mechanisms such as those described in Applicant's claims 20 and 21 could be used to verify an electronic item in an insecure environment. It is not clear how the teachings of Benson combined with the teachings of Shavit would render such mechanisms obvious, since even if one wished to combine these two references, there is no reasonable probability of success, since the use of the electronic item's inputs would not provide a mechanism to verify the content of the electronic item itself, unlike the mechanisms claimed by Applicant.

Claims 22-26 are dependent on claim 21, and are thus allowable for at least the reasons set forth above in connection with claim 21.

CONCLUSION

In view of the foregoing remarks, Applicants submit that this claimed invention is allowable over the references cited against this application. Applicants therefore request the entry of this Amendment, reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 14, 2004

By: _____
Andrew B. Schwaab
Reg. No. 38,611

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, L.L.P.
1300 I Street, NW
Washington, D.C. 20005
(202) 408-4000

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service's "Express Mail Post Office to Addressee" service under 37 CFR § 1.10, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 14, 2004. Express Mail Label No.: EV 527339428 US

Signed: _____
Andrew B. Schwaab

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

W. Olin Sibert

Application No.: 09/628,692

Filed: July 28, 2000

For: SYSTEMS AND METHODS FOR USING CRYPTOGRAPHY TO PROTECT SECURE AND INSECURE COMPUTING ENVIRONMENTS

Group Art Unit: 2136

Examiner: Karl G. Colin

Confirmation No.: 3388

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

PETITION FOR EXTENSION OF TIME

Applicant hereby petition for a three month extension of time to reply to the Office Action mailed January 14, 2004. Please charge the fee of $950.00 to our Deposit Account No. 06-0916.

Please grant any extensions of time required to enter this response and charge any additional required fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 14, 2004

By: _____
Andrew B. Schwaab
Reg. No. 38,611

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, L.L.P.
1300 I Street, NW
Washington, D.C. 20005
(202) 408-4000